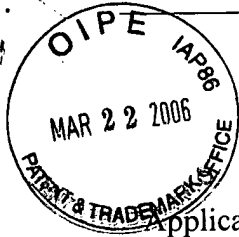


Please Direct All Correspondence to Customer Number **20995****TRANSMITTAL LETTER****APPEAL BRIEF**

Applicant : Peter Ford  
App. No : 09/463,146  
Filed : April 14, 2000  
For : ENCRYPTED BROADCAST  
MESSAGES IN A CELLULAR  
COMMUNICATIONS SYSTEM  
Examiner : Benjamin E. Lanier  
Art Unit : 2132

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

March 20, 2006  
(Date)

John M. Carson, Reg. No. 34,303

**Mail Stop Appeal Brief - Patents**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

Transmitted herewith for filing in the above-identified application are the following enclosures:

- (X) On Appeal To The Board of Patent Appeals and Interferences Appeal Brief in (19) pages.

**FILING FEES:**

FEE CALCULATION				
FEE TYPE		FEE CODE	CALCULATION	TOTAL
Appeal Brief	41.20(b)(2)	1402 (\$500)		\$500
1 Month Extension	1.17(a)(1)	1251 (\$120)		\$120
			<b>TOTAL FEE DUE</b>	<b>\$620</b>

- (X) An extension of time is hereby requested by payment of the appropriate fee indicated above.
- (X) A check in the amount of **\$620** is enclosed.
- (X) Return prepaid postcard.

Docket No. : EIP7.001APC/E208.USw

**Customer No.: 20,995**

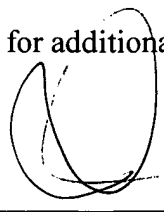
Application No. : 09/463,146

Filing Date : April 14, 2000

---

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Dated: March 20, 2006



---

John M. Carson  
Registration No. 34,303  
Attorney of Record  
Customer No. 20,995  
(619) 235-8550

2457651  
031706



EIP7.001APC/E208 LARK

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Appellant : Peter Ford  
Appl. No. : 09/463,146  
Filed : April 14, 2000  
For : ENCRYPTED BROADCAST  
MESSAGES IN A CELLULAR  
COMMUNICATIONS SYSTEM  
Examiner : Benjamin E. Lanier  
Group Art Unit : 2132

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Mail Stop Appeal Brief -- Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

March 20, 2006

(Date)

John M. Carson, Reg. No. 34,303

**ON APPEAL TO THE BOARD OF PATENT APPEALS AND INTERFERENCES**  
**APPEAL BRIEF**

Mail Stop Appeal Brief -- Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief relates to an appeal to the Board of Patent Appeals and Interferences of the final rejection set forth in a final Office Action mailed August 11, 2005, in the above-captioned application.

03/22/2006 MBIZUNES 00000036 09463146

01 FC:1401 500.00 OP  
02 FC:1251 120.00 OP

Void date: 03/22/2006 MBIZUNES  
03/22/2006 MBIZUNES 00000036 09463146  
01 FC:1401 -500.00 OP

03/22/2006 MBIZUNES 00000066 09463146

01 FC:1402 500.00 OP

Appl. No. : 09/463,146  
Filed : April 14, 2000



**TABLE OF CONTENTS**

I. REAL PARTY IN INTEREST.....	3
II. RELATED APPEALS AND INTERFERENCES .....	3
III. STATUS OF CLAIMS.....	3
IV. STATUS OF AMENDMENTS .....	3
V. SUMMARY OF CLAIMED SUBJECT MATTER .....	3
VI. ISSUES TO BE REVIEWED ON APPEAL.....	5
VII. APPELLANT'S ARGUMENT .....	6
A. Claims 19-20, 24-25 and 27-37 are Patentable over Diachina, in view of Chaney .....	6
B. Claims 21-23 are Patentable over Diachina, in view of Chaney, and further in view of Farrugia.....	11
C. Conclusion .....	12
VIII. CLAIMS APPENDIX.....	12
IX. EVIDENCE APPENDIX.....	12
X. RELATED PROCEEDINGS APPENDIX .....	12

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

### **I. REAL PARTY IN INTEREST**

The real party in interest in this appeal is the assignee of this application, Orange Personal Communications Services, Ltd.

### **II. RELATED APPEALS AND INTERFERENCES**

Appellant is unaware of any related appeals or interferences.

### **III. STATUS OF CLAIMS**

The application was originally filed with a preliminary amendment canceling Claims 1-18 and adding Claims 19-37. In response to a first Office Action mailed on February 11, 2004, Claims 19, 21-22, 24, 28-29, 32, 34, and 37 were amended. In response to a second Office Action mailed on September 13, 2004, Claims 19, 21-22, 24, 28-29, 32 and 37 were amended, and Claim 26 was cancelled.

In a third and Final Office Action mailed on August 11, 2005, the Examiner finally rejected Claims 19-25 and 27-37.

### **IV. STATUS OF AMENDMENTS**

All offered amendments have been entered. Thus, Claims 19-25 and 27-37 appear before the Board as they were finally rejected, and the claims are attached hereto as Appendix A.

### **V. SUMMARY OF CLAIMED SUBJECT MATTER**

As described in the application as filed, embodiments of the invention include a method and apparatus for distributing information to users in a cellular telecommunications network. *See Application at p. 1, ll. 1-5.*

Claim 19 recites method of distributing information to users in a cellular telecommunications network comprising a plurality of base stations transceiving in a plurality of cells of the network. *See Application at p. 5, l. 21 through p. 6, l. 15; Figure 2.* The method includes providing a plurality of mobile stations, wherein each said mobile station is provided with a removable module which is capable of being used in association with any of a plurality of said mobile stations, each of the mobile stations having an associated information access status for the receipt of messages broadcast on a common channel of at least one cell of said network. *Id.; see also Application at p. 7, ll. 16-21; Figures 1, 2, 5.* The method also provides for enabling first mobile stations having a first information access status to decrypt and present the

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

message to a user in unencrypted form, by providing each removable module of each of the first mobile stations with a decryption function arranged to use a decryption key. *See Application at p. 12, l. 8 to p. 13, l. 14; p. 14, l. 21 through p. 15, l. 2; Figures 3, 4, 7.* The method further includes preventing second mobile stations having a second information access status from presenting the message in unencrypted form to a user when being served in the cell. *See Application at p. 24, ll. 1-10.* The method also comprises broadcasting a signal on a common channel of at least one cell of the network, the signal containing a limited access message in encrypted form, for general reception in the at least one cell and for limited access by users of the first mobile stations. *See Application at p. 10, ll. 1-8; p. 11, ll. 12-20; Figures 4-5.* The method additionally comprises transmitting a transfer protocol identifier indicating that the encrypted broadcast message is of a type for data download to the removable module from the first mobile station. *See Application at p. 22, ll. 8-15.* The method further includes, for each said first mobile station, passing the encrypted broadcast message to its corresponding removable module in response to receipt of the transfer protocol identifier. *See Application at p. 23, ll. 7-9.* The method also provides, for each removable module of each of the first mobile stations, decrypting said encrypted broadcast message using the decryption key in response to receipt of the encrypted broadcast message. *See Application at p. 23, ll. 9-16.* The method also comprises, for each said removable module, passing the decrypted broadcast message to its corresponding first mobile station for display thereon. *Id.*

Claim 32 recites a mobile station for receiving information in a cellular telecommunications system which includes means for receiving an encrypted message broadcast on a common channel of a cell of the cellular telecommunications system. *Application at p. 5, l. 21 through p. 6, l. 15; p. 7, ll. 16-21; Figures 1, 2, 5.* The mobile station also includes a means responsive to receipt of a transfer protocol identifier indicating that the broadcast message is of a type for data download to a removable module from the mobile station and configured to pass the encrypted broadcast message to the removable module, the removable module comprising a memory for storing a decryption function arranged to use a decryption key. *See Application at p. 22, ll. 9-15; p. 23, ll. 4-16; Figure 1, 2, 9.* The mobile station also comprises display means for displaying the message, when decrypted, to a user, wherein, in response to receipt of the encrypted broadcast message, the removable module decrypts the encrypted broadcast message

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

using the decryption key, and the display means displays the decrypted message to the user. *See Application at p. 7, ll. 16-21; p. 23, ll. 9-16; Figure 2.*

Claim 37 recites a mobile station for receiving information in a cellular telecommunications system which includes a receiver unit configured to receive an encrypted message broadcast on a common channel of a cell of the cellular telecommunications system. *See Application at p. 5, l. 21 through p. 6, l. 15; p. 7, ll. 16-21; Figures 1, 2, 5.* The mobile station further includes a processor responsive to receipt of a transfer protocol identifier indicating that the broadcast message is of a type for data download to a removable module from the mobile station. *See Application at p. 22, ll. 9-15; p. 23, ll. 4-16; Figure 1, 2, 9.* The mobile station also has a display to display the message, when decrypted, to a user. *See Application at p. 7, ll. 16-21; p. 23, ll. 9-16; Figure 2.* The mobile station further comprises a removable module comprising a memory for storing a decryption function arranged to use a decryption key, wherein in response to receipt of said encrypted broadcast message, the processor passes the message to the removable module, wherein the removable module decrypts said encrypted broadcast message using said decryption key, and wherein the mobile station displays the decrypted message to the user. *Id.; Application at p. 23, ll. 4-16; Figure 1, 2, 9.*

## **VI. ISSUES TO BE REVIEWED ON APPEAL**

This Appeal turns on the following issues:

(1) Claims 19-20, 24-25 and 27-37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over WO 96/41493 to Diachina, in view of U.S. Pat. No. 5,852,290 to Chaney.

(2) Claims 21-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Diachina, in view of Chaney, and further in view of Farrugia et al., "Smart Card Technology Applied to the future of European Cellular Telephone on the digital D-Network."

Appl. No. : 09/463,146  
Filed : April 14, 2000

## **VII. APPELLANT'S ARGUMENT**

### **A. Claims 19-20, 24-25 and 27-37 are Patentable over Diachina, in view of Chaney**

#### **1. The Examiner's Grounds for Rejection**

##### **a. Claims 19, 32, and 37**

The Examiner's rejection of each of independent Claims 19, 32, and 37 was stated as follows:

Referring to claims 19, 20, 24-25, 27-30, 32-34, 36, and 37, Diachina discloses controlling digital control channels for broadcast SMS wherein SMS messages can be encrypted to support different classes of messaging service (access status). Based on appropriate fee payments, a subscriber would be able to decrypt SMS message [sic] of varying classes (preventing and allowing information access, first, second information access status). Upon payment the mobile stations of the subscribers would be provided with the encryption keys for the SMS messages via over [sic] the air methods of manual entry of smart cards (removable module) into the mobile stations (Page 40, lines 5-27). Diachina does not specify that the message decryption takes place in the smart cards. Chaney discloses a smart card access control system for use in cellular communication wherein the smart cards of the cellular phones are used to decrypt messages (Col. 13, lines 17-24). It would be have been to one of ordinary skill in the art at the time the invention was made for the smart cards of Diachina to decrypt message [sic] because Diachina discloses that the messages are decrypted using processing means of the mobile stations (Page 40, lines 18-20), and when the smart cards are inserted in the mobile stations, they become processing means for the mobile station.

*Final Office Action at p. 4.* Although Claim 26 had been canceled by amendment, and the features recited in the claim had been incorporated into Claims 19, 32 and 37, the Examiner addressed this specific feature separately, in rejecting canceled Claim 26:

Referring to claim 26, Diachina discloses that the SMS messages contain header information that discloses from which channel the mobile terminal can download the SMS message (page 33).

*Final Office Action at p. 4.* Because Claim 19 has been amended to recite features similar to those recited in previously examined and now canceled Claim 26, the Examiner's rejection of Claim 26 will be discussed in reference to amended Claim 19.



**2. The Legal Standard**

To establish a prima facie case of obviousness, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings, and the prior art references, when combined, must teach or suggest all the claim limitations. M.P.E.P. § 2143 (emphasis added). Also, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).

**3. The Combination of Diachina and Chaney Fails to Show the Feature of a Transfer Protocol Identifier as Recited in Independent Claim 19 (and Similarly in Independent Claims 32 and 37)**

Each of independent Claims 19, 32, and 37 recites the feature of a message including "a transfer protocol identifier indicating that the encrypted broadcast message is of a type for data download". Each of these claims further recite the feature of "passing said encrypted broadcast message to its corresponding removable module in response to receipt of said transfer protocol identifier." Applicant submits that neither Diachina nor Chaney teaches or suggests the use of either of these features.

**a. Header Information as Disclosed in Diachina Does Not Teach or Suggest Indicating that the "Message Is Of A Type For Data Download to the Removable Module"**

As noted above, the Examiner stated that Diachina "discloses that the SMS messages contain header information that discloses from which channel the mobile terminal can download the SMS message." More particularly, the Examiner's rejection states that the feature of the message being *of a type for data download to a removable module* as recited in Claim 19 is met by Diachina because it "discloses that the SMS messages contain header information that discloses from which channel the mobile terminal can download the SMS message." Office Action at 4 (emphasis added). However, the Examiner failed to demonstrate how "header information" that indicates a download channel can constitute "a transfer protocol identifier indicating that the encrypted broadcast message is of a type for data download to the removable module" as recited in Claim 19 (and similarly in Claims 32 and 37).

Diachina, at page 33 line 8, states that header information is provided with every SMS frame, and that the header information describes the sub-channelling of the broadcast SMS

Appl. No. : 09/463,146  
Filed : April 14, 2000

channel. The sub-channelling information described in Diachina, however, does not indicate that the message is *of a type for data download to a removable module* as recited in Claim 19. Indeed, the header information in Diachina describes the location from which an SMS message can be downloaded. In contrast, Claim 19 recites a “transfer protocol identifier indicating that the encrypted broadcast message is of a type for data download to the removable module.” Thus, the transfer protocol identifier in Claim 19 is associated with the destination location of the downloaded data, while the header information in Diachina is associated only with the location from which the data could be downloaded. Thus, the entire purpose and effect of the header information described in Diachina is very different from the “transfer protocol identifier” recited in Claim 19.

In relation to the feature of “a removable module”, Diachina describes there being a smart card: “[E]ncryption keys or algorithms could be sent to the mobiles ... via a ‘smart card’, for example.” *Diachina at page 40, lines 23-25*. Consequently, in order for Diachina to teach the claimed feature of a “transfer protocol identifier indicating that the encrypted broadcast message is of a type for data download to the removable module,” the “header information” (which is alleged to be the ‘transport protocol identifier’) must indicate that the broadcast message is of a type for data download to the smartcard. However, as explained above, the header information in Diachina does not include any indication that the encrypted broadcast message is of a type for download to the smartcard. Rather, and to reiterate, the header information merely includes information regarding sub-channeling of the broadcast SMS channel. *See, e.g., Diachina, p. 33, l. 8-21*. Applicant therefore submits that the header information described in Diachina, along with a mere mention of the use of a smartcard to send encryption keys, cannot properly be construed as teaching or suggesting “transmitting a transfer protocol identifier indicating that the encrypted broadcast message is of a type for data download to the removable module from the first mobile station; for each said first mobile station, passing said encrypted broadcast message to its corresponding removable module in response to receipt of said transfer protocol identifier”, as recited in Claim 19.

**b. Chaney Does Not Cure Diachina’s Deficiencies Regarding Indicating that the “Message Is Of A Type For Data Download to the Removable Module”**

The Examiner attempts to rely upon Chaney to supplement the deficiencies in Diachina without fully defining, in terms of features in claim 19, what these deficiencies are. In fact, and

Appl. No. : 09/463,146  
Filed : April 14, 2000

because the Examiner has not examined each feature of claim 19 with respect to Diachina, the system described in Chaney, even if properly combinable with Diachina, is not alleged by the Examiner to teach or suggest, nor does it in fact teach or suggest, at least the feature of a “transfer protocol identifier indicating that the encrypted broadcast message is *of a type for data download to the removable module*” as recited in Claim 19.

c. **Header Information as Disclosed in Diachina Does Not Teach or Suggest “Passing Said Encrypted Broadcast Message to Its Corresponding Removable Module In Response to Receipt of Said Transfer Protocol Identifier”**

Diachina also fails to teach or suggest the feature of “passing said encrypted broadcast message to its corresponding removable module in response to receipt of said transfer protocol identifier” as recited in Claim 19 (and similarly in Claims 32 and 37).

The Examiner points to nothing in Diachina which purports to show that broadcast messages are passed to a removable module “in response to receipt of” the header information (which is alleged to be a “transport protocol identifier”). Diachina describes a communications system wherein the decryption of SMS messages is carried out by processing units in mobile stations. *Page 40, lines 17-20*. The processing units described in Diachina are not removable modules, but rather are part of the mobile station. *See Figure 4 (showing processing unit 180 as being part of mobile station 120)*. Thus, decryption of broadcast messages in Diachina’s system occurs in the mobile equipment itself rather than in the smartcard. This is because encrypted broadcast messages in Diachina’s system are not passed to a removable module (i.e., a smartcard). To the extent, if any, that passing of encrypted messages occurs in response to receiving “header information,” Diachina only describes passing messages to processing units, which cannot be considered to be a “removable module” as recited in Claim 19.

d. **Chaney Does Not Cure Diachina’s Deficiency Regarding “Passing Said Encrypted Broadcast Message ... In Response to Receipt of Said Transfer Protocol Identifier”**

Chaney describes a smart-card based access control system for a video signal processing system, such as a pay-TV system. *Chaney at col. 3, lines 39-56*. In a first embodiment described by Chaney, a signal processing system includes a tuner 100 coupled to a forward error corrector (FEC) 110, wherein the FEC 110 is configured to convert the analog output of the tuner 100 to a digital signal. *Col. 4, lines 26-27, 32-35; Figure 1*. A transport unit 120 is coupled to the FEC 110 and is configured to detect and separate types of data in the tuned signal. *Col. 3, lines 36-37*.

Appl. No. : 09/463,146  
Filed : April 14, 2000

The tuned signal includes data packets, and each packet includes a header with data defining the sub-stream with which the packet is associated. *Col. 4, lines 43-48*. In this first embodiment described by Chaney, the transport unit 120 extracts and processes header data and directs video and audio data to demux/descrambler 130 for descrambling and demultiplexing into video and audio signals. *Col. 5, lines 36-49; Figure 1*.

In contrast to Chaney's first embodiment, Claim 19 recites a method wherein an encrypted broadcast message is passed to a removable module in response to receipt of a transfer protocol identifier, where the broadcast message is decrypted. The scrambled video and audio data in Chaney's first embodiment are not descrambled in a removable module or smart card. Thus, even if the header data in Chaney is considered to be a "transport protocol identifier," the first embodiment described by Chaney does not cure the defects of Diachina because the broadcast message is not passed to the *removable module* in *response to receipt* of the header data described in Chaney.

In a second embodiment described by Chaney, a smart-card 180 includes an IC 181 with a descrambler unit 185 and is issued with both an entitlement control message (ECM) key and an entitlement management message (EMM) key stored in memory 423. *Col. 7, lines 15-16; col. 11, lines 8-23, 35-44; Figures 1, 4*. The ECM key is used to descramble ECM data, which is stored in memory 424 and used by a CPU 421 to generate video and audio keys for use in descrambling video and audio data. *Col. 11, lines 45-59*. The descrambler 185 includes a transport decode unit 472, for providing functions similar to the functions of the transport unit 120 in the first embodiment, including processing header data. *Col. 7, lines 61-64; col. 8, lines 5-6*. Scrambled or encrypted video and audio data is descrambled at the descrambling unit 478 on the smart card 180. *Col. 8, lines 25-41; col. 12, lines 20-26*.

Thus, in the second embodiment described by Chaney, the *smart card* both processes packet header data *and* descrambles encrypted audio and video data. In contrast to Chaney's second embodiment, the *mobile stations* in Claim 19 receive a transfer protocol identifier and pass the encrypted broadcast message to the removable module *in response to receipt of the transfer protocol identifier*. Accordingly, even if packet header data in Chaney were considered to include a "transport protocol identifier" as recited in Claim 19, Chaney's second embodiment fails to cure the defects of Diachina because the packet header data, together with the encrypted audio and video data, are passed to the smart card prior to processing of the header. Thus any

Appl. No. : 09/463,146  
Filed : April 14, 2000

actions taken *in response to receipt of the header data* are actions other than passing the encrypted data to the removable module.

**e. Claims 19, 32, and 37 are Thus Patentable**

Therefore, as neither Diachina nor Chaney, either alone or in combination, teach or suggest every element as recited in Claim 19, Applicant respectfully submits that Claim 19 is in condition for allowance.

As noted above, Claims 32 and 37 recite features similar to those recited in the method of Claim 19, the arguments with respect to Claim 19 similarly apply to Claims 32 and 37, and thus, Claims 32 and 37 are respectfully submitted for further review as patentable subject matter.

Because Claims 20-25 and 27-31 depend from Claim 19 and Claims 33-36 depend from Claim 32, pursuant to 35 U.S.C. § 112, ¶ 4, they incorporate by reference all the limitations of the claim to which they refer. It is therefore submitted that these claims are in condition for allowance at least for the reasons expressed with respect to the independent claim, and for their other features.

**B. Claims 21-23 are Patentable over Diachina, in view of Chaney, and further in view of Farrugia**

**1. The Examiner's Grounds for Rejection**

In rejecting Claims 21-23, the Examiner relied on his rejection of independent Claim 19 as described above, and further stated as follows:

Diachina does not disclose storing the keys on the smart cards in an encrypted form. Farrugia discloses the use of smart card technology with cellular networks where the key used to decrypt encrypted cellular message [sic] are stored in an encrypted fashion on the smart card of the subscribers [sic] module (Page 101). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the keys of Diachina on the smart cards in order to control access to the keys as taught by Farrugia.

*Final Office Action at p. 5.*

**2. The Legal Standard**

To establish a *prima facie* case of obviousness, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings, and the prior

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

art references, when combined, must teach or suggest all the claim limitations. M.P.E.P. § 2143 (emphasis added). Also, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). If a proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the claims are not sufficient to render the claims prima facie obvious. MPEP 2343.01; *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). Moreover, if a proposed modification would render the prior art unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *Id.*, *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

**3. Pursuant to 35 U.S.C. § 112, ¶ 4, Claims 21-23 are Patentable**

Claims 21-23 depend from Claim 19. Therefore, pursuant to 35 U.S.C. § 112, ¶ 4, they incorporate by reference all the limitations of the claim to which they refer. It is thus submitted that these claims are in condition for allowance at least for the reasons expressed with respect to the independent claims as discussed above.

**C. Conclusion**

In view of the foregoing arguments, Appellant respectfully submits that Claims 19-25 and 27-37 are patentable over the prior art of record.

**VIII. CLAIMS APPENDIX**

Attached hereto as a **Claims Appendix** is a copy of finally rejected Claims 19-25 and 27-37 in the present case.

**IX. EVIDENCE APPENDIX**

Also attached is an **Evidence Appendix** for inclusion of evidence and indicating no evidence is included.

**X. RELATED PROCEEDINGS APPENDIX**

Also attached hereto is a **Related Proceedings Appendix** for inclusion of information regarding related proceedings and indicating no information regarding related proceedings is included.

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP



Dated: March 20, 2006

By: \_\_\_\_\_  
John M. Carson  
Attorney of Record  
Registration No. 34,303  
Customer No. 20,995  
(619)235-8550

**CLAIMS APPENDIX**  
(Claims as finally rejected)

Claims 1-18 (canceled)

19. (Previously Presented) A method of distributing information to users in a cellular telecommunications network comprising a plurality of base stations transceiving in a plurality of cells of the network, the method comprising:

providing a plurality of mobile stations, wherein each said mobile station is provided with a removable module which is capable of being used in association with any of a plurality of said mobile stations, each of the mobile stations having an associated information access status for the receipt of messages broadcast on a common channel of at least one cell of said network;

enabling first mobile stations having a first information access status to decrypt and present the message to a user in unencrypted form, by providing each removable module of each of said first mobile stations with a decryption function arranged to use a decryption key;

preventing second mobile stations having a second information access status from presenting the message in unencrypted form to a user when being served in the cell;

broadcasting a signal on a common channel of at least one cell of the network, the signal containing a limited access message in encrypted form, for general reception in the at least one cell and for limited access by users of said first mobile stations;

transmitting a transfer protocol identifier indicating that the encrypted broadcast message is of a type for data download to the removable module from the first mobile station;

for each said first mobile station, passing said encrypted broadcast message to its corresponding removable module in response to receipt of said transfer protocol identifier;

for each said removable module of each of said first mobile stations, decrypting said encrypted broadcast message using said decryption key in response to receipt of said encrypted broadcast message; and

for each said removable module, passing said decrypted broadcast message to its corresponding first mobile station for display thereon.



**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

20. (Previously Presented) The method according to Claim 19, further comprising enabling both the first and second mobile stations to read a message identifier comprised in the signal and accompanying a message.

21. (Previously Presented) The method according to Claim 19, further comprising storing the decryption key in the removable module in encrypted form.

22. (Previously Presented) The method according to Claim 21, further comprising decrypting the decryption key by the first mobile station using a data string specific to the removable module.

23. (Previously Presented) The method according to Claim 22, wherein the data string is a subscriber identifier used in the cellular telecommunications network.

24. (Previously Presented) The method according to Claim 19, further comprising transmitting the decryption key to the first mobile stations via a radio interface in the cellular telecommunications network.

25. (Previously Presented) The method according to Claim 19, wherein the removable module is a subscriber identity module.

26. (canceled)

27. (Previously Presented) The method according to Claim 19, further comprising storing in the removable module an application program for performing the decryption and for controlling a display of the message on the mobile station.

28. (Previously Presented) The method according to Claim 19, wherein the signal comprises a plurality of limited access messages each having a corresponding decryption key,

the method comprising providing the first mobile stations with the decryption keys, storing the decryption keys on removable modules of the first mobile stations, and enabling only ones of the first mobile stations having a decryption key corresponding to a limited access message to present the limited access message to a user in unencrypted form when being served in said cell.

29. (Previously Presented) The method according to Claim 28, further comprising providing each of the first mobile stations with a selection of the decryption keys in accordance with a subscription held for each first mobile station respectively.

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

30. (Previously Presented) The method according to Claim 19, wherein alternative limited access messages are broadcast in cells located in different areas of the cellular telecommunications network.

31. (Previously Presented) The method according to Claim 19, wherein the common channel is a cell broadcast channel of a GSM-type communications system.

32. (Previously Presented) A mobile station for receiving information in a cellular telecommunications system, the mobile station comprising:

means for receiving an encrypted message broadcast on a common channel of a cell of the cellular telecommunications system;

means responsive to receipt of a transfer protocol identifier indicating that the broadcast message is of a type for data download to a removable module from the mobile station and configured to pass said encrypted broadcast message to the removable module, said removable module comprising a memory for storing a decryption function arranged to use a decryption key ; and

display means for displaying the message, when decrypted, to a user, wherein, in response to receipt of said encrypted broadcast message, the removable module decrypts said encrypted broadcast message using said decryption key, and the display means displays the decrypted message to the user.

33. (Previously Presented) The mobile station according to Claim 32, wherein the removable module is a subscriber identity module.

34. (Previously Presented) The mobile station according to Claim 32, wherein the decryption function comprises an application program for performing the decryption and for controlling the display of the message on the mobile station.

35. (Previously Presented) The mobile station according to Claim 32, wherein the mobile station is configured to operate in accordance with GSM Phase 2+.

36. (Previously Presented) The mobile station according to Claim 32, wherein the mobile station is configured to operate as a cellular mobile telephone.

37. (Previously Presented) A mobile station for receiving information in a cellular telecommunications system, the mobile station comprising:

a receiver unit configured to receive an encrypted message broadcast on a common channel of a cell of the cellular telecommunications system;

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

a processor responsive to receipt of a transfer protocol identifier indicating that the broadcast message is of a type for data download to a removable module from the mobile station;

a display to display the message, when decrypted, to a user; and

a removable module comprising a memory for storing a decryption function arranged to use a decryption key, wherein in response to receipt of said encrypted broadcast message, the processor passes the message to the removable module, wherein the removable module decrypts said encrypted broadcast message using said decryption key, and wherein the mobile station displays the decrypted message to the user.

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

**EVIDENCE APPENDIX**

None

**Appl. No.** : **09/463,146**  
**Filed** : **April 14, 2000**

**RELATED PROCEEDINGS APPENDIX**

None

2457573  
031706